

DRAFT OF NEW DCID 1/16

CONTENTS

- * SIMPLIFIED 1ST SECTION DEALING WITH POLICY AND RESPONSIBILITIES AND EXEMPTIONS; FOLLOWED BY REQUIREMENTS (CHAPTER II).
- * "REQUIREMENTS" SECTION (CHAPTER II) COVERS NEW MODES TO REFLECT EXISTING ENVIRONMENT WITH MATRIX TO MAKE IT UNDERSTANDABLE.
- * EXEMPTIONS FOR "OPERATIONAL" TACTICAL/STRATEGIC ELEMENTS
- * NEW SECTION(S) DEALING WITH
 - ACQUISITIONS/PROCUREMENT STD'S
 - UNCLASSIFIED PROGRAM PROCESSING RELATED TO SOFTWARE DEVELOPMENT ACTIVITY
 - MOA'S BY MEMBER AGENCIES
 - "OVER THE COUNTER" ACCESS CONTROLS
 - AREA OF MAINTENANCE/SERVICE OF EQUIPMENT
 - WORD PROCESSING EQUIPMENT
 - PROVIDING DCI "FEEDBACK" ON STATE OF ACCREDITATIONS, EXEMPTIONS

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/16

SECURITY OF FOREIGN INTELLIGENCE

IN

AUTOMATED DATA PROCESSING SYSTEMS AND NETWORKS

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/16

SECURITY OF FOREIGN INTELLIGENCE IN AUTOMATED
DATA PROCESSING SYSTEMS AND NETWORKS

FOREWORD

This Directive, issued pursuant to Section 102 of the National Security Act of 1947, Executive Order 12036 and National Security Council Intelligence Directives, establishes policy and responsibilities, specifies exemption limitations and sets forth general requirements and minimum security requirements for National Foreign Intelligence Board (NFIB) member agencies and all other United States Government departments and agencies (hereinafter referred to as the Responsible Authority) processing or storing intelligence information in automated data processing systems and networks.

This directive requires the uniform protection of classified foreign intelligence and foreign counterintelligence involving sensitive intelligence sources and methods and applies equally when automated data processing systems and networks are owned or operated by the United States Government or by its contractors or consultants. *

Chapter I establishes Community policy and responsibilities, and specifies exemption limitations. Chapter II sets forth general requirements and minimum security requirements for automated data processing systems processing or storing classified foreign intelligence and counterintelligence information and Chapter III identifies the requirements for automated data processing networks which are formed by the interconnection of automated data processing systems.

* Foreign intelligence and foreign counterintelligence are used⁶⁵ in this Directive as defined in Section 45, Executive Order 12036 and as classified under the provisions of Executive Order 11652. For the purpose of this Directive, the term "intelligence information" includes both foreign intelligence and foreign counterintelligence as so defined.

CHAPTER I

Policy, Responsibilities and Exemptions

I.1 POLICY - Implementation and adherence to security standards for automated data processing (ADP) operations are necessary for the protection of classified foreign intelligence and foreign counterintelligence involving sensitive intelligence sources and methods. It is, therefore, Community policy that:

I.1.1 ADP security standards and capabilities in addition to those established by this Directive are encouraged and may be implemented if deemed appropriate by the individual NFIB member or Responsible Authority.

I.1.2 ADP systems and networks involving foreign governments shall be addressed on a case-by-case basis by the NFIB member(s) or Responsible Authority(ies) involved.

I.1.3 This Directive shall not apply to ADP systems or networks used exclusively to provide telecommunications services. Such systems and networks are controlled by existing pertinent National policies and regulations.

I.1.4 Nothing in this Directive shall supersede or augment the requirements on the control, use and dissemination of Restricted Data, formerly Restricted Data or Communications Security (COMSEC) related material as established by or under existing statutes, directives or Presidential policy.

I.2 RESPONSIBILITIES - Each NFIB member agency and Responsible Authority is responsible for:

I.2.1 Establishing a formal ADP security program in compliance with this Directive.


I.2.2 Ensuring compliance by his respective organization, and any other organization for which he has cognizant security responsibility, with the provisions of this Directive.

I.3 EXEMPTIONS - The NFIB member or Responsible Authority may:

I.3.1 Delegate his responsibility to a duly appointed designee except as specifically prohibited in Chapter II, Paragraph II.2d(1).

I.3.2 Temporarily exempt a specific ADP system or network under his jurisdiction from complete compliance with this Directive when such compliance would clearly and significantly impair execution of the assigned "Field" operational mission.

I.3.3 Under emergency "Field" operational conditions, temporarily exempt specific individuals with less than a TOP SECRET security clearance (based on a complete background investigation) to allow them access to an ADP system or network which is processing or storing Sensitive Compartmented Information (SCI).*



*would like to see this
as legal info, rather than
temporary patch*

* The term "Sensitive Compartmented Information" as used in this Directive includes all information and materials bearing special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products for which Community systems and compartmentation have been or will be formally established.

Page Denied

Next 10 Page(s) In Document Denied